COMMUNICATIONS
SECURITY
ESTABLISHMENT
COMMISSIONER

# Annual Report

2004-2005

Canada

Office of the Communications Security Establishment Commissioner
P.O. Box 1984
Station "B"
Ottawa, Ontario
K1P 5R5

Tel.: (613) 992-3044
Fax: (613) 992-4096

© Minister of Public Works and Government Services Canada 2005
ISBN 0-662-68995-X
Cat. No. D95-2205

Communications Security
Establishment Commissioner

The Right Honourable Antonio Lamer,
P.C., C.C., C.D., L.L.D., D.U.

CANADA

Commissaire du Centre de la
sécurité des télécommunications

Le très honorable Antonio Lamer,
c.p., c.c., c.d., L.L.D., d.u.

April 2005

Minister of National Defence
MGen G.R. Pearkes Building, 13th Floor
101 Colonel By Drive, North Tower
Ottawa, Ontario
K1A 0K2

Dear Sir:

Pursuant to subsection 273.63 (3) of the *National Defence Act*, I am pleased to submit to you my 2004-2005 annual report on my activities and findings, for your submission to Parliament.

Yours sincerely,

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

*This report is dedicated to the memory of*

# Kathryn Randle

1950-2004

Our first editor

105-04759/

# TABLE OF CONTENTS

Introduction ..... 1

The Year in Review ..... 2

2004-2005 Activities ..... 5

- The review process ..... 5
- Reviews under the Commissioner's general mandate ..... 6
- Reviews of activities under ministerial authorization ..... 7
- Review of past recommendations ..... 10
- 2004-2005 findings ..... 11
- Complaints and concerns about CSE activities ..... 12

The Commissioner's Office ..... 12

Shaping the Review Environment ..... 14

Concluding Thoughts ..... 15

Annex A: Mandate of the Communications Security Establishment Commissioner ..... 17

Annex B: Statement of Expenditures 2004-2005 ..... 19

Annex C: Classified Reports, 1996-2005 ..... 21

# INTRODUCTION

In the two years since my appointment as the Communications Security Establishment (CSE) Commissioner, an array of dramatic events has captured the world's attention, including the Cedar Revolution in Lebanon, and calls for the withdrawal of Syrian forces from that country, the Orange Revolution in the Ukraine, a renewed interest in the peace plan for Palestine, an election in Iraq, and parliamentary debates on equal rights for women in Kuwait. Meanwhile, Canada continues to deploy forces in Afghanistan so as to provide a secure environment suitable for the peaceful economic and political development of that nation. The positive scope of these political events is heartening.

Paralleling these changes in the geo-political landscape is the continued threat of terrorism globally. As evidenced by the bombings that killed or injured thousands in Madrid on March 11, 2004, international networks of terrorists continue to operate. This is the global environment in which CSE operates, one that is uncertain and volatile. At the same time, we are witnessing dramatic technological advances that, in the wrong hands, pose an ongoing threat to government information systems and assets, and ultimately, to Canada's security and economic competitiveness.

In the face of challenges such as these, CSE plays an essential role and makes a vital contribution to Canada's security and national interests. An integral part of Canada's security and intelligence community, CSE provides foreign intelligence to the Government of Canada and ensures the protection of the Government's electronic information and its information infrastructures. Today's national security realities make it imperative that CSE maintain its capacity and a high state of technological and operational readiness to meet Canada's evolving needs in these areas.

As the CSE Commissioner, my role is to determine if CSE's activities comply with the laws of Canada in general and, in particular, to assess whether CSE appropriately safeguards the privacy of Canadians. Over the past two years as Commissioner, I have gained an appreciation for the complex and important issues involved. Moreover, I can rely on the extensive expertise, loyalty and commitment of my staff to assist me in carrying out the Commissioner's review role effectively and efficiently.

I am pleased to submit this Annual Report for 2004-2005, summarizing the work of my office over the past year. As this report demonstrates, much has been accomplished during that time. More importantly, the report provides clear support for the essential role of the Commissioner's review function and the assurances it brings to Canadians.

## THE YEAR IN REVIEW

Largely as a result of the three-year review of Bill C-36, the omnibus *Anti-Terrorism Act*, there has been heightened attention over the past year to Canada's security and intelligence community, including CSE. When the Bill was enacted in December 2001, it resulted in key amendments to existing Acts. Of particular interest to my office were the amendments to the *Official Secrets Act* (now the *Security of Information Act)* and the *National Defence Act (NDA)*. The latter provided the legislative basis for CSE and this Office. Since December 2004, this omnibus legislation has been the subject of a required three-year review by committees of the House of Commons and the Senate. I will be watching the outcome of this review with keen interest.

A number of other activities initiated during 2004-2005 have the potential to significantly affect either my office or the broader security environment in which we operate. For example, last year saw a commitment by the Prime Minister to create a National Security Committee of Parliamentarians. This commitment was made in response to a proposal set out in Canada's first-ever national security policy, which was tabled in Parliament on April 27, 2004. In this regard, an Interim Committee of Parliamentarians was struck to examine the proposal. I appeared before this committee on September 8, 2004.

Of interest to my office as well are the deliberations and outcomes of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, chaired by Mr. Justice Dennis O'Connor. In addition to investigating the role of Canadian officials in Mr. Arar's deportation from the United States to Syria, the Commission is examining options for review mechanisms for certain activities of the RCMP. I responded to the opportunity to make a submission to the Commission about some of the review options put forward. In my submission, I identified the relative strengths and weaknesses of each approach and made a recommendation on how best to proceed, given the need to safeguard the rights of persons in Canada, the realities of today's security environment and the highly sensitive nature of the RCMP's activities.

In my opinion, the most effective and logical approach is to establish one review mechanism to examine activities of the RCMP. This model would recognize the unique mandate of the RCMP, provide for a corresponding review body with the required expertise, and limit the changes required to the two organizations directly affected, the RCMP and the existing Public Complaints Commission. Furthermore, implementing this

structure would not affect other organizations or review groups in Canada's security and intelligence community where change in my respectful view is neither sought after nor required.

That being said, the Arar Commission's goal will be to strike an appropriate balance that is in the best interests of Canada. Again, I will be watching the deliberations with interest.

I had expressed concerns in last year's annual report about two legislative proposals: Bill C-7, the *Public Safety Act, 2002*, which introduced legislative amendments on a range of subjects, from transportation safety and immigration to biological weapons; and Bill C-14, which proposed amendments to the *Criminal Code* and the *Financial Administration Act*, among others. The concerns I had initially expressed about this legislation were later addressed. I am satisfied that, as passed, the legislation establishes uniform responsibility and accountability for all departments for the protection of their computer systems and networks.

Bill C-11, the so-called *whistle-blower* legislation, was first introduced as Bill C-25 on March 22, 2004, but to date has not been passed by Parliament. Although CSE is exempt from such legislation, passage of the Bill would place an onus on CSE to establish a parallel system, with a possible review role for the Commissioner. Obviously, this legislation is of interest to me and I will continue to monitor its progress in Parliament, as well as any response by CSE.

## 2004-2005 ACTIVITIES

Each year, my office undertakes extensive reviews of CSE activities in areas that were identified as priorities as part of a multi-year workplan. Most often, these are areas within the intelligence production cycle where there is the potential for privacy issues to be raised. I report to the Minister of National Defence on all my reviews, either to provide assurance of the lawfulness of CSE activities or to bring his attention to specific concerns that arise as a result of the reviews. My activity as Commissioner properly remains confined to *ex post* review, and not to oversight, which entails a role in relation to CSE's ongoing activities.

During 2004-2005, I submitted a total of five classified reports to the Minister – two under my general review mandate and the remainder in compliance with my mandate to review specific activities authorized by the Minister.

### The review process

As in all my work, I place a high priority on collaboration during the review process. In practice, this means sharing any concerns with relevant personnel in CSE at the earliest possible stage so that appropriate corrective action can be taken, if required. As part of my office's efforts to effect change in a timely way, my staff now provide a summary briefing to all concerned CSE personnel following the review process.

One of the underlying principles guiding review is the anticipation of problem areas before they arise. That means looking beyond the issue of whether an unlawful activity has occurred, to whether one might occur and what measures can be put in place to prevent it. I believe this type of proactive and preventive approach is essential in balancing the undisputable need for security and intelligence activities with the fundamental privacy rights we have come to expect in Canada.

## Reviews under the Commissioner's general mandate

In the period covered by this report, I submitted two classified reports to the Minister of National Defence on subjects related to my general mandate[1] to review CSE's activities to ensure they conform with the law.

One of the reports involved a review of an operational program conducted by CSE under the authority of subsection 273.64(1)(a) of the *NDA*, often referred to as CSE's foreign intelligence mandate. In this instance, my findings indicated that CSE had acted lawfully in respect of this program. Moreover, employees assigned to this program demonstrated knowledge and awareness of the relevant law and policy that governed it.

The other classified report to the Minister concerned my review of a subset of activities conducted by CSE under the authority of subsection 273.64(1)(c) of the *NDA*, in response to requests for assistance received from federal law enforcement agencies.[2] In this regard, the RCMP is CSE's primary client. When providing assistance to the RCMP, the scope of which is limited and defined in policy, CSE does so as an agent. Before agreeing to act in that capacity, however, CSE must first satisfy itself that the RCMP is authorized to make the request and then be satisfied that it has the authority to provide the assistance the RCMP has requested.

My office examined CSE's assistance to the RCMP under mandate (c) for the year 2003. Based on the activities reviewed, CSE's assistance was found to be in compliance with the law.

---

[1] See Annex A.

[2] 273.64(1) The mandate of the Communications Security Establishment is:
(c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

That being said, however, both reports included recommendations, many of which concerned certain weaknesses in CSE's policies and procedures, an area that has drawn similar attention and mention in previous reviews. I have also recommended that CSE accelerate efforts to improve and update existing information and records management systems. At the time of writing, CSE had resolved some of these issues and had committed to address the remainder in the coming months.

## Reviews of activities under ministerial authorization (MA)

As stated, it is my practice to conduct *ex post* review. In the case of CSE's MA-related activities, my reviews are undertaken once the authorizations in question expire.

My focus for the year under review was on activities conducted by CSE under the authority of three MAs, all of which concerned foreign intelligence collection and were the subject of classified reports to the Minister.

In conducting review activities for MAs, my office is guided directly by the legislation, which dictates what activities CSE can and cannot undertake. Specifically, my reviews in this area focus on the interception of private communications, which is what an MA authorizes. A private communication is defined in section 183 of the *Criminal Code* as

> ... any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone

> communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it…

For the purpose of foreign intelligence collection, the *NDA* authorizes CSE to intercept private communications as long as the interception was the result of its having directed activities at a foreign entity located outside Canada. Over the past two years, I have focused much of my attention on foreign intelligence MAs because of their broad scope and potential degree of intrusiveness on the privacy of Canadians. While information technology security (ITS) MAs also authorize the interception of private communications, CSE seeks such authority in every instance at the request of the client agency whose systems and networks are being verified.

In my last annual report, I observed that a number of my concerns had been resolved, while some others remained. During this past year, I have been able to bring clarity to points of law and interpretation with respect to CSE's activities conducted under the authority of these provisions. My office engaged in discussions with staff and officials at CSE throughout this process.

For jurists who are accustomed to dealing with warrants issued by judges, a foreign intelligence MA is a strange sort of creature. However, one must take into account that, when collecting foreign intelligence, CSE is directing its interception efforts at foreign communications, or at least at the foreign end of communications, and a warrant issued by a Canadian court has no jurisdiction outside Canada in this instance.

Foreign intelligence MAs are a unique solution to an equally unique set of circumstances that can arise when CSE recognizes that an intercepted communication either leads into or flows out of Canada. While the interception has not been directed at a communication in Canada, one end of the communication is in Canada and is therefore, by law, a *private communication*. If this communication contains information essential to international affairs, defence or security, as specified in CSE's legislation, it is reasonable that the Government of Canada would want CSE to retain and report on it.

The foreign intelligence MA provisions in Part V.1 of the *NDA* include four conditions that must be met before the Minister of National Defence will authorize the interception of a private communication. I am of the opinion that their inclusion is both reasonable and consistent with other legislation that establishes an authority to engage in activities that would, in the absence of adequate justification, be judged an infringement on the rights of individuals as protected by the *Charter of Rights and Freedoms*.

In my view, these MA provisions are an exception to Part VI of the *Criminal Code* that protects against the invasion of privacy. I have no doubt as to their purpose because the *NDA* explicitly authorizes the interception of private communications subject to the threshold established by the four conditions, and to ministerial review. From my examination of private communications intercepted by CSE, I am able to determine if CSE has met the conditions imposed in the MA – for example, I know if the interception was a result of activities directed at a foreign entity outside of Canada. I can also determine if the communication was lawfully used, retained or destroyed – that is to say, whether or not it was

essential to the international affairs, defence or security of Canada.

In light of the above, I believe my review of activities that CSE has conducted under a foreign intelligence MA must focus on the intercepted private communications that CSE identifies to me as having been recognized and retained during the term of the authorization.

The Minister of National Defence is aware of how I have interpreted and will continue to discharge my mandate in respect of foreign intelligence MAs. I have also provided the Minister with my interpretation of the MA provisions, as currently written, and what they allow for in law. Further, I have made specific suggestions as to what could be done to remove ambiguities and to ensure a common understanding of the operational application of these provisions.

## Review of past recommendations

There is substantial evidence that I believe supports my office's review function and the impact it has had on CSE's internal processes over the years. When warranted by the review findings, I may include recommendations for action on the part of CSE. My recommendations are, appropriately, non-binding. Binding recommendations would usurp the prerogative of both the Minister, who has overall responsibility for CSE, and of the Chief of CSE, who is responsible under Part V.1 of the *NDA* for the management and control of the organization. However, one of the concerns with a review body whose recommendations are non-binding is whether that review is effective or not. I can say with confidence that review works, based on my experience with CSE's response to the recommendations made by my office.

As I outlined in my previous annual report, last year we began a process to track CSE's response to the recommendations my predecessor and I made in

classified reports submitted to the Minister of National Defence since 1996. I am pleased to provide an update. A process has also been put in place to ensure a timely response to recommendations made in upcoming reports from my office.

Over the past year, my staff worked closely with CSE to monitor their response and subsequent actions with respect to the recommendations – including establishing timetables and target dates for completion. Of the 77 recommendations made from 1996 to the end of the current fiscal year, the majority have been accepted and implemented, and I am awaiting what I believe will be a positive response from CSE on a number of others. Many of the recommendations address broad policy issues such as formalizing relations, while others focus on technical and operational practices, including ensuring consistent definitions and appropriate accountability structures. That being said, the ultimate goal of all recommendations I make is to prevent conditions or practices that have the potential to lead to unlawfulness or that could affect the privacy of Canadians. I believe that this tracking process for recommendations is fundamental to achieving this goal.

I commend the Chief of CSE on the extent to which he has accepted review as an integral part of the vision for his organization. As well, I would like to express my appreciation to CSE for their co-operation and willingness to monitor the recommendations.

## 2004-2005 findings

Each year, I state my findings about the lawfulness of CSE's activities based on the reviews my office has conducted over the past year. I am able to report that I am satisfied that the CSE activities examined during the period under review complied with the law. Moreover, I am satisfied that the intercepted private communications I examined were lawfully acquired, used and retained.

## Complaints and concerns about CSE Activities

Under Paragraph 273.63 (2)(b) of the *National Defence Act*, I am required to respond to a complaint by undertaking any investigation I consider necessary to determine whether CSE is engaging in unlawful activity. At various fora, people have expressed their surprise at the limited number of complaints directed toward my office over the years.

To my mind, the likelihood of a public complaint is diminished by the nature and focus of CSE's activities, which are technology-based and directed at foreign entities outside Canada. Unlike other federal intelligence or law enforcement agencies, CSE neither has a public profile nor engages in activities that place it in the public domain. During 2004-2005, I received no complaints about CSE activities from any source.

# THE COMMISSIONER'S OFFICE

The reviews that my office conducts are in-depth and multi-faceted, taking months to complete. I place great importance on ensuring that they are carried out with methodological rigour and consistency. Last year, I requested an internal study of my office's own review processes and I am satisfied that it employs the full range of appropriate analytical and investigative review methodologies that are best practices in the public and private sectors. Briefings, multi-level interviews, the examination of a broad range of hard and soft copy records holdings, (including authorities, policies, legal opinions and operational files), legal research, inter-agency consultation and debriefing sessions are just some of the elements that constitute this process.

During the past year, my staff also upgraded its electronic record-keeping system, known as RDIMS (records/document information management system). It is designed to improve the security, retention and access to both

non-electronic and electronic documents. This has enhanced my office's ability to track and manage its internal records.

In support of the review function, my office maintains a full-time working staff of eight, as well as a complement of contract professionals who bring a range of expertise and experience in a variety of related fields. For example, some of my staff have had considerable exposure to Canada's security and intelligence community; others have special expertise in information technology, research, policy development and communications. As a result of a multi-phase staffing initiative that was completed in June 2004, my office has been operating at full strength for almost a year. I do not anticipate further staffing requirements in the near future, provided the tempo of activity remains unchanged.

To ensure that my staff stays connected to and engaged in the broader issues facing the security and intelligence community, we host informal presentations by representatives of government and academia working in the security field. Last year, on five occasions, we invited presenters to speak about, and share in discussions on, Canadian intelligence priorities in such subject areas as terrorism, information technology and the law, and privacy.

As part of my efforts to ensure awareness of the role of the Commissioner, last year my staff – at CSE's invitation – began to give presentations to new CSE employees as part of their orientation course. This contributes directly to CSE's fulfillment of the Ministerial Directive on Accountability Framework, which is designed to ensure that CSE personnel are aware of the Commissioner's mandates of *determining whether those activities (of CSE) are in compliance with the law and of investigating complaints by citizens,*

*including CSE employees, or permanent residents of Canada concerning the lawfulness of such activities.* The Chief of CSE is also directed to ensure CSE employees extend *full support and cooperation* to the Commissioner in carrying out his mandate.

In the interests of sharing expertise and learning about timely issues, my staff attended two conferences in October 2004: the International Intelligence Review Agencies Conference (IIRAC) in Washington D.C., and the annual Canadian Association for Security Intelligence Studies (CASIS) in Ottawa. In March 2005, I was invited to participate in a symposium on Counter-terrorism and the Law held at the University of Ottawa. While I declined to be a member of the panel, I took the opportunity offered me to address the participants, and I offered a few thoughts for their consideration. In addition, and for the second year, one of my staff will participate in the National Security Studies Seminar organized by the Canadian Forces College and planned for April. These events allow for the exchange of ideas and information on issues of mutual interest and concern, and help to keep us abreast of developments in the world that affect intelligence and review.

During the past year, my office's annual expenditures were $966,781. I am able to report that, once again, I discharged my mandated activities within budget. Annex B to this report provides a statement of my office's expenditures.

## SHAPING THE REVIEW ENVIRONMENT

It goes without saying that Canada's security and intelligence sector – as well as its various review mechanisms – will be shaped by the important parliamentary and government initiatives currently underway. As discussed earlier in this report, the ongoing three-year review of the omnibus

*Anti-Terrorism Act*, the recommendations on review mechanisms for the RCMP that are anticipated from the Arar Commission and the proposed National Security Committee of Parliamentarians, all have the potential to make a substantial impact on the security and intelligence sector over the coming months and years.

As CSE Commissioner, I will continue to monitor these initiatives carefully and, wherever possible, make a positive contribution to the outcomes. I believe that the review community has much to offer and I welcome the opportunity to be part of the process. One of the principles guiding my input will be the need for a thoughtful approach to these issues, one that does not attempt to change what works, merely for the sake of change itself. While changes may certainly be called for, we must take care not to dilute what Parliament has put in place without due consideration and reflection.

## CONCLUDING THOUGHTS

Despite the fact that the past year has posed many challenges, I look back upon it with no small degree of satisfaction. It has been a successful year. Addressing certain ambiguities in law in respect of CSE's activities under Ministerial authorizations, and establishing how my office will increase its effectiveness in reviewing them, for example, are positive steps. I am heartened by the number of recommendations made since the creation of my office that CSE has accepted and implemented, and by the ongoing dialogue between CSE and ourselves.

On a broader note, I am fully persuaded that review agencies such as my own can make an important contribution to the ongoing debate between the considerations of security and of privacy. Western democracies must make difficult choices as to where to draw the line at a time when asymmetric

threats are a part of our reality, and it is not an easy debate.

At a recent symposium on Counter-terrorism and the Law held at the University of Ottawa, and referred to earlier, my former colleague Supreme Court Justice Ian Binnie raised questions for discussion by the panel. He observed that the greatest threat to our rule of law is terrorism, and in matters of security it is absolutely necessary for the courts to show deference to state agencies because they have more expertise, information and resources on such matters than the courts. He questioned, however, at what point this deference should stop. While I do not have an easy answer to Mr. Justice Binnie's question, I know that it is one that merits serious contemplation given the challenges our contemporary society faces.

## Mandate of the Communications Security Establishment Commissioner

*National Defence Act – Part V.1*

"**273.63** (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.

(2) The duties of the Commissioner are

(a) to review the activities of the Establishment to ensure that they are in compliance with the law;

(b) in response to a complaint, to undertake any investigation that the Commissioner considers necessary; and

(c) to inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.

(3) The Commissioner shall, within 90 days after the end of each fiscal year, submit an annual report to the Minister on the Commissioner's activities and findings, and the Minister shall cause a copy of the report to be laid before each House of Parliament on any of the first 15 days on which that House is sitting after the Minister receives the report.

(4) In carrying out his or her duties, the Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*.

(5) The Commissioner may engage the services of such legal counsel, technical advisers and assistants as the Commissioner considers necessary for the proper performance of his or her duties and, with the approval of the Treasury Board, may fix and pay their remuneration and expenses.

(6) The Commissioner shall carry out such duties and functions as are assigned to the Commissioner by this Part or any other Act of Parliament, and may carry out or engage in such other related assignments or activities as may be authorized by the Governor in Council.

(7) The Commissioner of the Communications Security Establishment holding office immediately before the coming into force of this section shall continue in office for the remainder of the term for which he or she was appointed.

"**273.65** (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization issued under this section to ensure that they are authorized and report annually to the Minister on the review."

*Security of Information Act*

"**15.** (1) No person is guilty of an offence under section 13 or 14 if the person establishes that he or she acted in the public interest.

"**15.** (5) A judge or court may decide whether the public interest in the disclosure outweighs the public interest in non-disclosure only if the person has complied with the following:

"**15.** (5) (b) the person has, if he or she has not received a response from the deputy head or the Deputy Attorney General of Canada, as the case may be, within a reasonable time, brought his or her concern to, and provided all relevant information in the person's possession to,

(ii) the Communications Security Establishment Commissioner, if the person's concern relates to an alleged offence that has been, is being or is about to be committed by a member of the Communications Security Establishment, in the purported performance of that person's duties and functions of service for, or on behalf of, the Communications Security Establishment, and he or she has not received a response from the Communications Security Establishment Commissioner within a reasonable time."

## Statement of Expenditures 2004-2005

### Standard Object Summary

| | |
|---|---|
| Salaries and Wages | 514,130 |
| Transportation and Telecommunications | 20,688 |
| Information | 18,293 |
| Professional and Special Services | 216,889 |
| Rentals | 142,454 |
| Purchased Repair and Maintenance | 105 |
| Materials and Supplies | 8,581 |
| Acquisition of Machinery and Equipment | 45,464 |
| Other Expenditures | 177 |
| **Total** | **$966,781** |

## Classified Reports, 1996-2005

Classified Report to the Minister
– March 3, 1997 (TOP SECRET)

Classified Report to the Minister
– Operational Policies with Lawfulness Implications – February 6, 1998 – (SECRET)

Classified Report to the Minister
– CSE's Activities under *** – March 5, 1998 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
– Internal Investigations and Complaints – March 10, 1998 (SECRET)

Classified Report to the Minister
– CSE's activities under *** – December 10, 1998 (TOP SECRET/CEO)

Classified Report to the Minister
– On controlling communications security (COMSEC) material – May 6, 1999 (TOP SECRET)

Classified Report to the Minister
– How We Test (A classified report on the testing of CSE's signals intelligence collection and holding practices, and an assessment of the organization's efforts to safeguard the privacy of Canadians) – June 14, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
– A Study of the *** Collection Program – November 19, 1999 (TOP SECRET Codeword/CEO)

Classified Report to the Minister
– On *** – December 8, 1999 (TOP SECRET/COMINT)

Classified Report to the Minister
– A Study of the *** Reporting Process – an overview (Phase I) – December 8, 1999 (SECRET/CEO)

Classified Report to the Minister
– A Study of Selection and *** – an overview – May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** – follow-up – May 10, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- Internal Investigations and Complaints – follow-up – May 10, 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program – June 15, 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review – September 14, 2000 (TOP SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process – Phase II *** – April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
- A study of the *** Reporting Process – Phase III *** – April 6, 2001 (SECRET/CEO)

Classified Report to the Minister
- CSE's participation *** – August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's support to *** as authorized by *** and *** – August 20, 2001 (TOP SECRET/CEO)

Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – August 21, 2002 (SECRET)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** – November 13, 2002 (TOP SECRET/CEO)

Classified Report to the Minister
- CSE's SIGINT activities carried out under the *** 2002 *** Ministerial authorization – November 27, 2002 (TOP SECRET/CEO)

Classified Report to the Minister
– Lexicon – 26 March 2003 (TOP SECRET/COMINT)

Classified Report to the Minister
– CSE's activities pursuant to three XXX Ministerial authorizations including *** *** – May 20, 2003 (SECRET)

Classified Report to the Minister
– CSE's support to XXX, as authorized by *** and code named *** – Part I – November 6, 2003 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
– CSE's support to XXX, as authorized by *** and code named *** – Part II – March 15, 2004 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
– A review of CSE's activities conducted under XXX Ministerial authorization – March 19, 2004 (SECRET/CEO)

Classified Report to the Minister
– Internal investigations and complaints – follow-up – March 25, 2004 (TOP SECRET/CEO)

Classified Report to the Minister
– A review of CSE's activities conducted under XXX Ministerial authorization – April 19, 2004 (SECRET/CEO)

Classified Report to the Minister
– Review of CSE XXX Operations under Ministerial authorization – June 1, 2004 (TOP SECRET/COMINT)

Classified Report to the Minister
– CSE's Support to XXX – January 7, 2005 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
– External Review of CSE's XXX Activities Conducted Under Ministerial authorization – February 28, 2005 (TOP SECRET/COMINT/CEO)

Classified Report to the Minister
– A Study of the XXX Collection Program – March 15, 2005 (TOP SECRET/COMINT/CEO)

Commissaire
du Centre
de la sécurité
des télécommunications

# Rapport annuel

2004-2005

Canada

Bureau du Commissaire du Centre de la sécurité des télécommunications
C.P. 1984, Succursale « B »
Ottawa (Ontario)
K1P 5R5

Tél. : (613) 992-3044
Téléc. : (613) 992-4096

© Ministre des Travaux publics et des Services gouvernementaux Canada 2005
ISBN 0-662-68995-X
N° de cat. D95-2005

Commissaire du Centre de la
sécurité des télécommunications

Le très honorable Antonio Lamer,
c.p., c.c., c.d., L.L.D., d.u.

CANADA

Communications Security
Establishment Commissioner

The Right Honourable Antonio Lamer,
P.C., C.C., C.D., L.L.D., D.U.

Avril 2005

Ministre de la Défense nationale
Édifice Mgén G.R. Pearkes, 13e étage
101, promenade Colonel By, tour nord
Ottawa (Ontario)
K1A 0K2

Monsieur le Ministre,

Conformément au paragraphe 273.63 (3) de la *Loi sur la défense nationale*, j'ai le plaisir de vous soumettre mon rapport annuel pour l'année 2004-2005, qui fait état de mes activités et constatations, aux fins de présentation au Parlement.

Je vous prie d'agréer, Monsieur le Ministre, l'assurance de ma haute considération.

Antonio Lamer

P.O. Box/C.P. 1984, Station "B"/Succursale « B »
Ottawa, Canada
K1P 5R5
(613) 992-3044 Téléc. : (613) 992-4096

*Ce rapport est dédié à la mémoire de*

# Kathryn Randle

1950-2004

notre première rédactrice

# TABLE DES MATIÈRES


Introduction ..... 1

Rétrospective de l'année ..... 2

Activités de 2004-2005 ..... 5

- Le processus d'examen ..... 6
- Examens effectués dans le cadre du mandat général du commissaire ..... 6
- Examens d'activités découlant d'une autorisation ministérielle ..... 8
- Examen de recommandations passées ..... 11
- Constatations faites en 2004-2005 ..... 13
- Plaintes et préoccupations relatives aux activités du CST ..... 13

Le bureau du commissaire ..... 13

Modeler le contexte d'examen ..... 16

Dernières réflexions ..... 17

Annexe A : Mandat du commissaire du Centre de la sécurité des télécommunications ..... 19

Annexe B : État des dépenses de 2004-2005 ..... 21

Annexe C : Rapports classifiés, 1996-2005 ..... 23

# INTRODUCTION

Au cours des deux années qui se sont écoulées depuis ma nomination au poste de commissaire du Centre de la sécurité des télécommunications (CST), une série d'événements dramatiques ont capté l'attention du monde, entre autres la révolution des cèdres au Liban et les demandes de retrait des forces syriennes de ce pays, la révolution orange en Ukraine, un intérêt renouvelé pour le plan de paix pour la Palestine, les élections en Iraq, et les débats parlementaires sur l'égalité des droits des femmes au Koweït. Entre-temps, le Canada a continué de déployer des forces en Afghanistan afin de ménager un environnement sûr, propice au développement économique et politique pacifique de ce pays. La portée positive de ces événements politiques est encourageante.

La menace continue de terrorisme à l'échelle mondiale fait pendant à cette évolution du contexte géopolitique. Comme en témoignent les attentats à la bombe qui ont tué ou blessé des milliers de personnes à Madrid, le 11 mars 2004, les réseaux internationaux de terroristes continuent d'opérer. C'est dans ce contexte mondial incertain et volatil que le CST exerce ses activités. Parallèlement, nous sommes témoins de progrès technologiques spectaculaires qui, s'ils tombaient dans de mauvaises mains, présenteraient une menace permanente pour les systèmes et les fonds d'information du gouvernement et, en fin de compte, pour la sécurité et la compétitivité économique du Canada.

Face à de tels défis, le CST joue un rôle essentiel et apporte une contribution capitale à la sécurité et aux intérêts nationaux du Canada. Le CST, qui fait partie intégrante de la collectivité canadienne de la sécurité et du renseignement, fournit des renseignements étrangers au gouvernement du Canada et assure la protection des renseignements électroniques de l'État et de son infrastructure

d'information. Compte tenu des réalités actuelles de la sécurité nationale, il est impératif que le CST conserve sa capacité et un haut degré de préparation technologique et opérationnelle pour répondre aux besoins changeants du Canada dans ces domaines.

En ma qualité de commissaire du CST, mon rôle consiste à déterminer si les activités du Centre respectent les lois du Canada en général et, en particulier, à évaluer s'il protège convenablement la vie privée des Canadiens. Dans l'exercice de mes fonctions au cours des deux dernières années, j'ai pu apprécier la complexité et l'importance des questions en cause. Je peux par ailleurs compter sur les connaissances étendues, la loyauté et le dévouement de mon personnel pour m'aider à m'acquitter de mon rôle d'examen de manière efficace et efficiente.

Je suis heureux de présenter ce rapport annuel pour 2004-2005, qui résume le travail accompli par mon bureau au cours de l'année écoulée. Comme ce document le révèle, ce travail a été considérable. Chose plus importante, il appuie clairement le caractère essentiel de la fonction d'examen du commissaire et les assurances qu'elle apporte aux Canadiens.

## RÉTROSPECTIVE DE L'ANNÉE

Au cours de l'année écoulée, on a prêté une attention accrue à la collectivité canadienne de la sécurité et du renseignement, dont le CST, en grande partie par suite de l'examen triennal du projet de loi omnibus C-36, ou *Loi antiterroriste*. L'adoption du projet de loi, en décembre 2001, a entraîné des modifications fondamentales de lois existantes qui avaient toutes pour but de renforcer la capacité du Canada de combattre le terrorisme. Mon bureau était particulièrement intéressé par les modifications de la *Loi sur les secrets officiels* (désormais *Loi sur la protection de l'information*)

et de la *Loi sur la défense nationale (LDN)*. Cette dernière a fourni le fondement législatif du CST et de mon bureau. Depuis décembre 2004, la loi omnibus fait l'objet d'un examen triennal obligatoire par des comités de la Chambre des communes et du Sénat. Je me pencherai avec un vif intérêt sur les résultats de cet examen.

Un certain nombre d'autres activités entreprises au cours de l'année 2004-2005 pourraient avoir une incidence importante sur mon bureau ou sur le contexte plus général de la sécurité dans lequel nous œuvrons. Par exemple, le Premier ministre s'est engagé, l'année dernière, à créer un comité de parlementaires sur la sécurité nationale. Il a pris cet engagement en réponse à une proposition figurant dans la toute première politique sur la sécurité nationale du Canada, qui a été déposée au Parlement le 27 avril 2004. Un comité provisoire de parlementaires avait été constitué pour examiner cette proposition. J'ai comparu devant ce comité le 8 septembre 2004.

Les délibérations et les conclusions de la Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, présidée par M. le juge Dennis O'Connor, intéressent également mon bureau. En plus d'enquêter sur le rôle des fonctionnaires canadiens relativement à l'expulsion de M. Arar des États-Unis en Syrie, la Commission examine différents mécanismes qui permettraient de contrôler certaines activités de la GRC. J'ai eu l'occasion de présenter un mémoire à la Commission au sujet de certaines des options proposées. J'y ai recensé les forces et les faiblesses relatives de chaque approche et fait une recommandation sur la meilleure façon de procéder, compte tenu de la nécessité de protéger les droits des personnes se trouvant au Canada, des réalités du contexte actuel de la

sécurité et de la nature très délicate des activités de la GRC.

À mon avis, l'approche la plus efficace et la plus logique consiste à établir un mécanisme de contrôle unique des activités de la GRC. Ce modèle reconnaîtrait le mandat singulier de celle-ci, prévoirait un organe d'examen correspondant possédant l'expertise nécessaire et limiterait les modifications à apporter aux deux organisations directement concernées, soit la GRC et l'actuelle Commission des plaintes du public. De plus, l'instauration de cette structure ne toucherait pas d'autres organisations ni groupes d'examen de la collectivité canadienne du renseignement et de la sécurité où des changements ne sont ni recherchés ni nécessaires.

Cela dit, la Commission Arar s'efforcera de trouver un équilibre adéquat, qui servira au mieux les intérêts du Canada. Ici encore, je suivrai les délibérations avec intérêt.

Dans mon rapport de l'année dernière, j'avais exprimé des préoccupations au sujet de deux mesures législatives proposées, soit le projet de loi C-7, *Loi de 2002 sur la sécurité publique*, qui prévoyait des modifications législatives sur plusieurs sujets, de la sécurité des transports à l'immigration en passant par les armes biologiques, et le projet de loi C-14, qui prévoyait entre autres des modifications du *Code criminel* et de la *Loi sur la gestion des finances publiques*. Ces préoccupations initiales ont été prises en compte par la suite, et je suis persuadé que les lois adoptées prévoient une responsabilité et une responsabilisation uniformes pour tous les ministères en ce qui concerne la protection de leurs systèmes et de leurs réseaux informatiques.

Le projet de loi C-11 (la loi dite de la dénonciation) a initialement été déposé sous le nom de projet de loi C-25 le 22 mars 2004, mais il n'a pas encore été adopté par le Parlement. Cette loi ne vise pas le CST, mais, si elle était adoptée, le Centre serait obligé d'établir un système parallèle qui devrait peut-être être soumis à l'examen du commissaire. Manifestement, ce projet de loi m'intéresse, et je continuerai de surveiller son cheminement au Parlement, ainsi que toute réaction du CST.

## ACTIVITÉS DE 2004-2005

Chaque année, mon bureau procède à des examens approfondis des activités du CST dans des domaines désignés prioritaires dans un plan de travail pluriannuel. Le plus souvent, il s'agit de domaines touchant le cycle de production du renseignement où des questions de protection de la vie privée risquent d'être soulevées. Je rends compte de tous mes examens au ministre de la Défense nationale, soit pour l'assurer de la légalité des activités du CST, soit pour lui signaler des préoccupations particulières découlant des examens. Mon travail de commissaire se limite à juste titre à un examen *a posteriori*; je n'exerce pas de surveillance, ce qui supposerait un rôle relativement aux activités courantes du CST.

Au cours de l'année 2004-2005, j'ai présenté en tout cinq rapports classifiés au ministre, soit deux dans le cadre de mon mandat général et les trois autres conformément à mon mandat d'examiner des activités particulières autorisées par le ministre.

## Le processus d'examen

Comme dans tout mon travail, j'accorde une haute priorité à la collaboration au cours du processus d'examen. En pratique, cela veut dire faire part de mes préoccupations au personnel concerné du CST le plus tôt possible, afin que des mesures correctrices appropriées puissent être prises s'il y a lieu. Dans le cadre des efforts déployés par mon bureau pour effectuer des changements de manière opportune, mes collaborateurs donnent maintenant, à la suite du processus d'examen, une séance d'information sommaire à tout le personnel concerné du CST.

L'un des principes fondamentaux qui guident l'examen consiste à repérer les secteurs problématiques avant qu'un problème ne se manifeste. Ainsi il s'agit de chercher à savoir non seulement s'il y a eu activité illégale, mais encore si une telle activité serait possible et si des mesures préventives peuvent être mises en place pour la prévenir. Je pense que cette approche proactive et préventive est essentielle pour établir un équilibre entre le besoin indiscutable d'activités de sécurité et de renseignement et les droits fondamentaux à la vie privée que nous nous attendons à voir garantis au Canada.

## Examens effectués dans le cadre du mandat général du commissaire

Au cours de la période couverte par le présent rapport, j'ai présenté deux rapports classifiés au ministre de la Défense nationale sur des sujets liés à mon mandat général[1] d'examiner les activités du CST pour en vérifier la légalité.

L'un des rapports portait sur l'examen d'un programme opérationnel mis en œuvre par le CST en vertu de l'alinéa 273.64(1)*a)* de la *LDN*, souvent désigné comme le mandat du CST en matière de renseignement étranger. Dans ce cas, mes

[1] Voir l'annexe A.

constatations ont révélé que le CST avait agi légalement dans le cadre de ce programme. De plus, les employés affectés avaient montré qu'ils connaissaient bien la loi et la politique qui le régissent.

L'autre rapport classifié au ministre avait trait à mon examen d'un sous-ensemble d'activités menées par le CST en vertu de l'alinéa 273.64(1)*c)* de la *LDN*, pour répondre aux demandes d'aide reçues d'organismes fédéraux d'application de la loi[2]. À cet égard, la GRC est le principal client du CST. Lorsqu'il fournit à la GRC une aide dont la portée est limitée et définie dans une politique, le CST le fait à titre d'agent. Avant d'accepter d'agir à ce titre, il doit cependant s'assurer, d'une part, que la GRC est autorisée à faire la demande et, d'autre part, qu'il a le pouvoir de fournir l'aide en question.

Mon bureau a examiné l'aide fournie par le CST à la GRC en vertu du mandat c) pour l'année 2003. En se fondant sur les activités examinées, il a conclu que cette aide avait été conforme à la loi.

Cela dit, toutefois, les deux rapports contenaient des recommandations dont beaucoup avaient trait à certaines faiblesses des politiques et procédures du CST, domaine qui a fait l'objet d'une attention et de mentions semblables lors d'examens précédents. J'ai en outre recommandé que le CST accélère ses efforts pour améliorer et actualiser les systèmes actuels de gestion de l'information et des dossiers. Au moment de la rédaction du présent rapport, le CST avait résolu certaines de ces questions et s'était engagé à s'occuper des autres au cours des mois à venir.

---

[2] 273.64(1) Le mandat du Centre de la sécurité des télécommunications est le suivant :

c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.

## Examens d'activités découlant d'une autorisation ministérielle (AM)

Comme je l'ai dit, j'effectue des examens *a posteriori*. Dans le cas des activités du CST autorisées par le ministre, j'entreprends mes examens une fois que les autorisations en question arrivent à terme.

Au cours de l'année à l'étude, je me suis concentré sur les activités menées par le CST en vertu de trois AM; ces activités avaient toutes trait à la collecte de renseignements étrangers et ont fait l'objet de rapports classifiés au ministre.

Lorsqu'il examine des activités menées en vertu d'AM, mon bureau est guidé directement par la législation, qui prescrit les activités permises et interdites au CST. Plus précisément, mes examens dans ce domaine portent sur l'interception de communications privées, qui sont ce qu'une AM autorise. L'article 183 du *Code criminel* définit une communication privée comme suit :

> Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.

Aux fins de la collecte de renseignements étrangers, la *LDN* autorise le CST à intercepter des communications privées à condition que l'interception résulte d'activités par lesquelles il vise une entité étrangère située à l'extérieur du

Canada. Au cours des deux dernières années, j'ai accordé beaucoup d'attention aux AM sur les renseignements étrangers en raison de leur vaste portée et du degré possible d'immixtion dans la vie privée de Canadiens. Les AM relatives à la sécurité des technologies de l'information (STI) autorisent également l'interception de communications privées, mais le CST sollicite cette autorisation dans tous les cas à la demande de l'organisme client dont les systèmes et les réseaux font l'objet d'une vérification.

Dans mon dernier rapport annuel, je signalais qu'un certain nombre de mes préoccupations avaient été résolues, tandis que d'autres subsistaient. Au cours de la dernière année, j'ai pu faire clarifier des points de droit et d'interprétation relatifs aux activités que mène le CST en vertu de ces dispositions. Mon bureau a eu des entretiens avec des membres du personnel et des cadres du CST tout au long de ce processus.

Pour les juristes qui sont habitués aux mandats émis par des juges, une AM relative à des renseignements étrangers peut surprendre. Toutefois, il faut tenir compte du fait que, lorsqu'il recueille des renseignements étrangers, le CST cherche à intercepter des communications étrangères, ou au moins la portion étrangère de ces communications, et qu'un mandat délivré par un tribunal canadien n'a pas compétence en dehors du Canada dans ce cas.

Les AM relatives à des renseignements étrangers sont une solution unique que l'on applique à un ensemble également unique de circonstances qui peuvent survenir lorsque le CST reconnaît que l'origine ou la destination d'une communication interceptée se trouve au Canada. L'interception ne visait pas une communication au Canada, mais l'un des pôles de la communication se trouve au

Canada et est par conséquent, selon la loi, une *communication privée*. Si cette communication contient de l'information essentielle aux affaires internationales, à la défense ou à la sécurité, comme le précise la loi intéressant le CST, il est raisonnable que le gouvernement du Canada veuille que le CST la conserve et en fasse rapport.

Les dispositions relatives aux AM visant l'obtention de renseignements étrangers, qui figurent à la partie V.1 de la *LDN*, comprennent quatre conditions qui doivent être remplies avant que le ministre de la Défense nationale autorise l'interception d'une communication privée. Je suis d'avis que l'inclusion de ces conditions est à la fois raisonnable et compatible avec les autres lois qui établissent un pouvoir d'exercer des activités qui, en l'absence de justification suffisante, seraient considérées comme un empiétement sur les droits de la personne garantis par la *Charte canadienne des droits et libertés*.

À mon avis, ces dispositions sur les AM constituent une exception à la partie VI du *Code criminel*, qui protège contre l'intrusion dans la vie privée. Je n'ai aucun doute quant à leur but, car la *LDN* autorise explicitement l'interception de communications privées sous réserve des quatre conditions et de l'examen ministériel. Mon examen des communications privées interceptées par le CST me permet de déterminer s'il a satisfait aux conditions imposées dans l'AM; par exemple, je sais si l'interception a été le résultat d'activités visant une entité étrangère située à l'extérieur du Canada. Je peux également déterminer si la communication a été utilisée, conservée ou détruite conformément à la loi, c'est-à-dire si oui ou non elle était essentielle aux affaires internationales, à la défense ou à la sécurité du Canada.

À la lumière de ce qui précède, je pense que mon examen des activités menées par le CST en vertu d'une AM visant l'obtention de renseignements étrangers doit porter sur les communications privées interceptées dont le CST m'indique qu'elles ont été reconnues et conservées pendant la durée de l'autorisation.

Le ministre de la Défense nationale sait comment j'ai interprété et je continuerai de remplir mon mandat à l'égard des AM visant l'obtention de renseignements étrangers. J'ai par ailleurs fourni au ministre mon interprétation des dispositions relatives aux AM, telles qu'elles sont actuellement libellées, et de ce qu'elles permettent en droit. J'ai en outre présenté des suggestions particulières sur ce que l'on pourrait faire pour supprimer les ambiguïtés et assurer une compréhension commune de l'application de ces dispositions en pratique.

## Examen de recommandations passées

Je pense qu'il existe des preuves concluantes à l'appui de la fonction d'examen de mon bureau et de l'incidence qu'elle a eue sur les processus internes du CST au fil des ans. Lorsque les constatations de l'examen le justifient, j'inclus parfois des recommandations de mesures à prendre par le CST. Ces recommandations sont, comme il se doit, non obligatoires. Des recommandations obligatoires usurperaient à la fois la prérogative du ministre, qui a la responsabilité d'ensemble du CST, et celle du chef du CST, qui est responsable de la gestion du Centre en vertu de la partie V.1 de la *LDN*. L'efficacité de l'examen effectué par un organisme dont les recommandations ne sont pas obligatoires pourrait être mise en doute. Toutefois, en me fondant sur mon expérience de la réaction du CST aux recommandations faites par mon bureau, je peux affirmer avec assurance que l'examen est efficace.

Comme je le mentionnais dans mon rapport annuel précédent, nous avons entrepris l'année dernière un travail de suivi de la réaction du CST aux recommandations que mon prédécesseur et moi-même avions faites dans des rapports classifiés présentés au ministre de la Défense nationale depuis 1996. Je suis heureux de rendre compte de ce travail. Un processus a aussi été mis en place pour faire en sorte que le Centre donne rapidement suite aux recommandations que formulera mon bureau dans les rapports à venir.

Au cours de l'année dernière, mon personnel a travaillé étroitement avec les gens du CST pour surveiller leur réaction et les mesures prises à la suite des recommandations, notamment l'établissement de calendriers et de dates cibles d'achèvement. Sur les 77 recommandations faites entre 1996 et la fin de la présente année financière, la majorité ont été acceptées et mises en œuvre, et j'attends ce qui, je pense, sera une réponse positive du CST sur un certain nombre d'autres. Nombre de recommandations portent sur des grandes questions de principe comme l'officialisation des relations, tandis que d'autres touchent les pratiques techniques et opérationnelles, dont l'établissement de définitions uniformes et de structures de responsabilisation appropriées. Cela dit, le but final de toutes mes recommandations est de prévenir les situations ou les pratiques qui pourraient mener à l'illégalité ou avoir une incidence sur la vie privée des Canadiens. Je pense que ce processus de suivi des recommandations est fondamental pour atteindre ce but.

Je salue la mesure dans laquelle le chef du CST a accepté l'examen en tant que partie intégrante de la vision de son organisation. Je tiens en outre à exprimer ma reconnaissance aux gens du CST pour leur coopération et leur volonté de donner suite aux recommandations.

### Constatations faites en 2004-2005

Chaque année, je présente mes constatations au sujet de la légalité des activités du CST en me fondant sur les examens effectués par mon bureau au cours des 12 mois précédents. Je suis en mesure de rapporter que je suis persuadé que les activités du CST examinées au cours de la période visée ont été conformes à la loi. De plus, je suis convaincu que les communications privées interceptées que j'ai examinées avaient été acquises, utilisées et conservées légalement.

### Plaintes et préoccupations relatives aux activités du CST

Conformément à l'alinéa 273.63(2)*b)* de la *Loi sur la défense nationale*, je dois répondre à une plainte en effectuant toute enquête que je juge nécessaire pour déterminer si le CST se livre à une activité illégale. Sur des tribunes diverses, des gens ont exprimé leur surprise au sujet du nombre limité de plaintes adressées à mon bureau au fil des ans.

À mon sens, la probabilité d'une plainte du public est réduite du fait de la nature et de l'objet des activités du CST, qui se fondent sur la technologie et visent des entités étrangères situées à l'extérieur du Canada. Contrairement aux autres organismes fédéraux de renseignement ou d'application de la loi, le CST n'a aucune visibilité publique et il ne se livre pas non plus à des activités qui le placent dans le domaine public. Au cours de l'année 2004-2005, je n'ai reçu de plainte d'aucune source au sujet des activités du CST.

## LE BUREAU DU COMMISSAIRE

Les examens qu'effectue mon bureau sont approfondis et multidimensionnels, et ils exigent des mois de travail. Il est, à mon sens, très important de m'assurer qu'ils sont exécutés de manière rigoureuse et uniforme. L'année dernière, j'ai demandé une étude interne des propres processus d'examen de mon bureau, et je suis convaincu qu'il emploie toute la gamme des

méthodes d'examen analytiques et d'investigation appropriées qui constituent des pratiques exemplaires dans le secteur public comme dans le secteur privé. Les séances d'information, les entrevues à plusieurs niveaux, l'examen d'un grand nombre de fonds de dossiers imprimés et électroniques (dont les autorisations, les politiques, les avis juridiques et les dossiers opérationnels), la recherche juridique, la consultation entre organismes et les séances de comptes rendus ne sont que quelques-uns des éléments constitutifs de ce processus.

Au cours de l'année dernière, mon personnel a par ailleurs amélioré son système électronique de tenue de dossiers, ou SGDDI (système de gestion des dossiers, des documents et de l'information). Ce système est conçu pour améliorer la sécurité et la conservation des documents non électroniques et électroniques ainsi que l'accès à ceux-ci. Mon bureau a ainsi amélioré sa capacité de suivre et de gérer ses dossiers internes.

À l'appui de la fonction d'examen, mon bureau continue d'avoir à son service huit employés à plein temps ainsi qu'un effectif de professionnels engagés par contrat qui possèdent un bagage d'expertise et d'expérience dans divers domaines connexes. Par exemple, certains de mes collaborateurs ont eu de nombreux contacts avec la collectivité canadienne de la sécurité et du renseignement; d'autres possèdent des connaissances spécialisées en technologies de l'information, en recherche, en élaboration des politiques et en communications. Par suite d'une initiative de dotation en plusieurs étapes qui a été achevée en juin 2004, mon bureau fonctionne avec un plein effectif depuis près d'une année. Je ne prévois pas de nouveaux besoins en personnel dans un avenir rapproché, pourvu que le rythme d'activité reste inchangé.

Pour que les membres de mon personnel demeurent au courant des grandes questions auxquelles est confrontée la collectivité de la sécurité et du renseignement et continuent de se sentir concernés, nous invitons des représentants des services gouvernementaux et des universités travaillant dans le domaine de la sécurité à leur donner des présentations informelles. L'année dernière, nous avons accueilli à cinq reprises des conférenciers qui sont venus traiter et discuter des priorités canadiennes en matière de renseignement dans des domaines comme le terrorisme, la technologie de l'information et le droit, et la protection de la vie privée.

Dans le cadre de mes efforts pour faire connaître le rôle du commissaire, mon personnel a commencé l'année dernière – à l'invitation du CST – à donner des exposés aux nouveaux employés du CST dans le cadre de leur cours d'orientation. Cette initiative contribue directement à l'exécution de la directive ministérielle sur le cadre de responsabilisation, qui vise à assurer que le personnel du CST est au courant des mandats du commissaire de *déterminer si ces activités (du CST) sont conformes à la loi et d'enquêter sur les plaintes de citoyens, dont des employés du CST, ou de résidents permanents du Canada concernant la légalité de ces activités*. Le chef du CST a en outre pour instruction de veiller à ce que les employés du Centre apportent *un appui et une coopération complets* au commissaire dans l'exécution de son mandat.

Dans le but de communiquer leur expertise et leur savoir sur des questions d'actualité, des membres de mon personnel ont participé à deux conférences tenues en octobre 2004, soit la conférence internationale des organismes d'examen des activités de renseignement, à Washington (D.C.), et la conférence annuelle de l'Association canadienne pour l'étude du renseignement et de la sécurité

(CASIS), à Ottawa. En mars 2005, j'ai été invité à participer à un symposium sur l'antiterrorisme et le droit, tenu à l'Université d'Ottawa. J'ai refusé de faire partie du groupe d'experts, mais j'ai profité de l'occasion qui m'était offerte d'adresser la parole aux participants et j'ai soumis quelques réflexions à leur examen. De plus, pour la deuxième année, un de mes collaborateurs participera au Séminaire des études de sécurité nationale organisé par le Collège des Forces canadiennes, qui doit se tenir en avril. Ces activités favorisent l'échange d'idées et d'information sur des questions d'intérêt mutuel et contribuent à nous tenir au courant des faits nouveaux dans le monde, qui ont des incidences dans le domaine du renseignement et de l'examen.

Au cours de la dernière année, les dépenses de mon bureau ont été de 966 781 $. Je suis à même de signaler que je me suis de nouveau acquitté de mon mandat dans le cadre de mon budget. On trouvera à l'annexe B un état des dépenses de mon bureau.

## MODELER LE CONTEXTE D'EXAMEN

Il va sans dire que le secteur canadien de la sécurité et du renseignement – de même que ses divers mécanismes d'examen – sera modelé par les importantes initiatives parlementaires et gouvernementales actuellement en cours. Comme je le mentionne plus haut, l'examen triennal en cours de la *Loi antiterroriste*, les recommandations relatives aux mécanismes d'examen de la GRC qui, prévoit-on, seront formulées par la Commission Arar, et la proposition de création d'un comité de parlementaires sur la sécurité nationale pourraient tous avoir une incidence importante sur le secteur de la sécurité et du renseignement au cours des prochains mois et des prochaines années.

À titre de commissaire du CST, je continuerai de surveiller ces initiatives de près et, dans tous les cas où ce sera possible, d'apporter une contribution positive aux résultats. Je pense que la collectivité de l'examen a beaucoup à offrir, et je me réjouis d'avoir l'occasion de participer au processus. L'un des principes qui guidera mon apport sera l'importance d'un examen sérieux de ces questions, qui ne cherche pas à changer ce qui fonctionne bien pour le simple plaisir de changer. Des changements pourront certes être justifiés, mais nous devrons faire attention à ne pas diluer ce que le Parlement a mis en place, sans y avoir mûrement réfléchi.

## DERNIÈRES RÉFLEXIONS

Même si l'année écoulée a présenté de nombreux défis, je l'évoque avec beaucoup de satisfaction. Ça a été une année réussie, marquée de réalisations fructueuses. Ainsi, nous avons résolu certaines ambiguïtés de droit touchant les activités menées par le CST en vertu d'autorisations ministérielles et nous avons trouvé des moyens d'accroître l'efficacité avec laquelle mon bureau les examine. Je suis encouragé par le nombre de recommandations qui, depuis la création de mon bureau, ont été acceptées et mises en œuvre par le CST, ainsi que par le dialogue suivi entre celui-ci et notre équipe.

Dans un ordre d'idées plus général, je suis convaincu que les organismes d'examen comme le nôtre peuvent apporter une contribution importante au débat en cours sur les considérations de sécurité et de protection de la vie privée. Les démocraties occidentales doivent faire des choix difficiles et déterminer où fixer les limites à une époque où les menaces asymétriques font partie de la réalité. Ce n'est pas un débat facile.

Lors du récent symposium sur l'antiterrorisme et le droit tenu à l'Université d'Ottawa et dont je fais mention plus haut, mon ancien collègue de la Cour suprême, le juge Ian Binnie, a soumis des questions au groupe d'experts. Il a fait remarquer que la plus grande menace pour la primauté du droit dans notre société est le terrorisme et que, en matière de sécurité, les tribunaux doivent absolument s'en remettre aux organismes de l'État parce que ceux-ci possèdent plus de connaissances, d'information et de ressources que les tribunaux dans ce domaine. Il a cependant demandé jusqu'où cela devait aller. Je n'ai pas de réponse facile à lui donner, mais je sais que sa question mérite un examen sérieux mené en regard des défis que soulève la situation contemporaine.

## Mandat du commissaire du Centre de la sécurité des télécommunications

*Loi sur la défense nationale - Partie V.I*

« **273.63** (1) Le gouverneur en conseil peut nommer, à titre inamovible pour une période maximale de cinq ans, un juge à la retraite surnuméraire d'une juridiction supérieure qu'il charge de remplir les fonctions de commissaire du Centre de la sécurité des télécommunications.

(2) Le commissaire a pour mandat

(a) de procéder à des examens concernant les activités du Centre pour en contrôler la légalité;

(b) de faire les enquêtes qu'il estime nécessaires à la suite de plaintes qui lui sont présentées;

(c) d'informer le ministre et le procureur général du Canada de tous les cas où, à son avis, le Centre pourrait ne pas avoir agi en conformité avec la loi.

(3) Le commissaire adresse au ministre, dans les quatre-vingt-dix jours suivant la fin de chaque exercice, un rapport sur l'exercice de ses activités. Le ministre dépose le rapport devant chacune des chambres du Parlement dans les quinze premiers jours de séance de celle-ci suivant sa réception.

(4) Dans l'exercice de son mandat, le commissaire a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes*.

(5) Le commissaire peut retenir les services de conseillers juridiques ou techniques ou d'autres collaborateurs dont la compétence lui est utile dans l'exercice de ses fonctions; il peut fixer, avec l'approbation du Conseil du Trésor, leur rémunération et leurs frais.

(6) Le commissaire exerce les attributions que lui confèrent la présente partie et toute autre loi fédérale; il peut en outre se livrer à toute activité connexe autorisée par le gouverneur en conseil.

(7) La personne qui occupe, à l'entrée en vigueur du présent article, la charge de commissaire du Centre de la sécurité des télécommunications est maintenue en fonctions jusqu'à l'expiration de son mandat.

« **273.65** (8) Le commissaire du Centre de la sécurité des télécommunications est tenu de faire enquête sur les activités qui ont été exercées sous le régime d'une autorisation donnée en vertu du présent article pour en contrôler la conformité; il rend compte de ses enquêtes annuellement au ministre. »

*Loi sur la protection de l'information*

« **15.** (1) Nul ne peut être déclaré coupable d'une infraction prévue aux articles 13 ou 14 s'il établit qu'il a agi dans l'intérêt public.

« **15.** (5) Le juge ou le tribunal ne peut décider de la prépondérance des motifs d'intérêt public en faveur de la révélation que si la personne s'est conformée aux exigences suivantes :

« **15.** (5) (b) dans le cas où elle n'a pas reçu de réponse de l'administrateur général ou du sous-procureur général du Canada dans un délai raisonnable, elle a informé de la question, avec tous les renseignements à l'appui en sa possession :

(ii) soit le commissaire du Centre de la sécurité des télécommunications si la question porte sur une infraction qui a été, est en train ou est sur le point d'être commise par un membre du Centre de la sécurité des télécommunications dans l'exercice effectif ou censé tel de ses fonctions pour le compte de celui-ci, et n'en a pas reçu de réponse dans un délai raisonnable. »

## État des dépenses, 2004-2005

### Sommaire des articles courants

| | |
|---|---|
| Traitements et salaires | 514 130 |
| Transports et télécommunications | 20 688 |
| Information | 18 293 |
| Services professionnels et spéciaux | 216 889 |
| Location | 142 454 |
| Achat de services de réparation et d'entretien | 105 |
| Fournitures et approvisionnements | 8 581 |
| Acquisition de machines et de matériel | 45 464 |
| Autres charges | 177 |
| **Total** | **966 781 $** |

## Rapports classifiés de 1996 à 2005

Classified Report to the Minister
– 3 mars 1997 (TRÈS SECRET)

Classified Report to the Minister
– Operational Policies with Lawfulness Implications – 6 février 1998 – (SECRET)

Classified Report to the Minister
– CSE's activities under *** – 5 mars 1998 (TRÈS SECRET Mot codé/ Réservé aux Canadiens)

Classified Report to the Minister
– Internal Investigations and Complaints – 10 mars 1998 (SECRET)

Classified Report to the Minister
– CSE's activities under *** – 10 décembre 1998 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
– On controlling communications security (COMSEC) material – 6 mai 1999 (TRÈS SECRET)

Classified Report to the Minister
– How We Test (Rapport classifié sur la mise à l'essai des pratiques du CST en matière de collecte et de conservation de renseignements électromagnétiques, et évaluation des efforts de l'organisme pour sauvegarder la vie privée des Canadiens) – 14 juin 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
– A Study of the *** Collection Program – 19 novembre 1999 (TRÈS SECRET Mot codé/Réservé aux Canadiens)

Classified Report to the Minister
– On *** – 8 décembre 1999 (TRÈS SECRET/COMINT)

Classified Report to the Minister
– A Study of the *** Reporting Process – an overview (Phase I) – 8 décembre 1999 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
– A Study of Selection and *** – an overview – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's Operational Support Activities Under *** – follow-up – 10 mai 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Internal Investigations and Complaints – follow-up – 10 mai 2000 (SECRET)

Classified Report to the Minister
- On findings of an external review of CSE's ITS Program – 15 juin 2000 (SECRET)

Classified Report to the Minister
- CSE's Policy System Review – 14 septembre 2000 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process – Phase II *** – 6 avril 2001 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the *** Reporting Process – Phase III *** – 6 avril 2001 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's participation *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's support to ***, as authorized by *** and *** – 20 août 2001 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A study of the formal agreements in place between CSE and various external parties in respect of CSE's Information Technology Security (ITS) – 20 août 2002 (SECRET)

Classified Report to the Minister
- CSE's support to XXX as authorized by *** and code named *** – 13 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's SIGINT activities carried out under the *** 2002 *** ministerial authorization – 27 novembre 2002 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Lexicon – 26 mars 2003 (TRÈS SECRET/COMINT)

Classified Report to the Minister
- CSE's activities pursuant to three XXX ministerial authorizations including *** *** – 20 mai 2003 (SECRET)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** – Part I – N 6 novembre 2003 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

Classified Report to the Minister
- CSE's support to XXX, as authorized by *** and code named *** – Part II – 15 mars 2004 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

Classified Report to the Minister
- A review of CSE's activities conducted under XXX Ministerial authorization – 19 mars 2004 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Internal investigations and complaints – Follow-up – 25 mars 2004 (TRÈS SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- A review of CSE's activities conducted under XXX Ministerial authorization – 19 avril 2004 (SECRET/Réservé aux Canadiens)

Classified Report to the Minister
- Review of CSE XXX Operations under Ministerial authorization – 1er juin 2004 (TRÈS SECRET/COMINT)

Classified Report to the Minister
- CSE's Support to XXX – 7 janvier 2005 (TRÈS SECRET/COMINT/ Réservé aux Canadiens)

Classified Report to the Minister
- External Review of CSE's XXX Activities Conducted Under Ministerial authorization – 28 février 2005 (TRÈS SECRET/COMINT/Réservé aux Canadiens)

Classified Report to the Minister
- A Study of the XXX Collection Program – 15 mars 2005 (TRÈS SECRET/ COMINT/Réservé aux Canadiens)